


IBM Global Services



Policy Rules!


Building an Effective and Manageable Security Policy Framework

Steve Brown, CISSP-ISSMP
IBM Internet Security Systems

IBM Internet Security Systems
Ahead of the threat.™

10/17/2008 © 2008 IBM Corporation

Professional Security Services




Introduction

Steve Brown, CISSP-ISSMP
IBM ISS Professional Security Services
browncs@us.ibm.com

2 | 10/17/2008 © 2008 IBM Corporation

Professional Security Services



Session Agenda

- Policy?
- The problem
- The solution
- Where to start
- What is a policy framework
- The policy development process
- Implementation and Education

3 | 10/17/2008 © 2008 IBM Corporation

Professional Security Services

Why Policy?

Compliance begins with Policy

- What do auditors ask for?
- What do many regulations specifically require?
- What do security firms recommend?

4 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Why Policy?

Other benefits

- Addresses the root cause of many security problems
- Direction for project planning
- Consistent and measurable application of standards and processes across the organization
- Defined security roles and responsibilities
- Reduced liability
- Basis for accountability

▪ How about the ability to appropriately protect the organization?

5 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Why Policy?

Hopefully we can agree that security documentation is critically important to successful security management and regulatory compliance!

6 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

The problem

Most organizations have one of the following 5 problems with their security policies

7 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Problem Number One

8 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Problem Number Two

Scattered Policies

- Disparate between organizations or business units
- Written at different levels of detail
- Approved by local management but called "Company Policy"
- Only available within departments or small groups

9 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Problem Number Three

Insufficient or Poorly Defined Policies

- Just because a memo reads "New Policy On" does not make it a policy
- A policy that prohibits inappropriate web surfing or forces a password change every 90 days does not adequately cover the full scope data protection

10 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Problem Number Four

Unenforceable or Unsupported Policies

- Like any project or initiative, policies need to be supported and enforced by all levels of the organization
- Well written policies that never make it out of IT, are not endorsed by senior management, and/or are not communicated are not really useful policies

11 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Problem Number Five

Unmanageable Policies

- If your security policy manual is 300 pages long – it isn't manageable
- Changes to procedural details should not require a full re-issue of a company's security policy
- Certain components of an organization's security documentation library shouldn't be viewable by the entire organization
- Guess what? - Your senior leadership doesn't want to read and endorse your boring IT book several times a year

12 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

The Solution

Build an effective and manageable information security policy framework

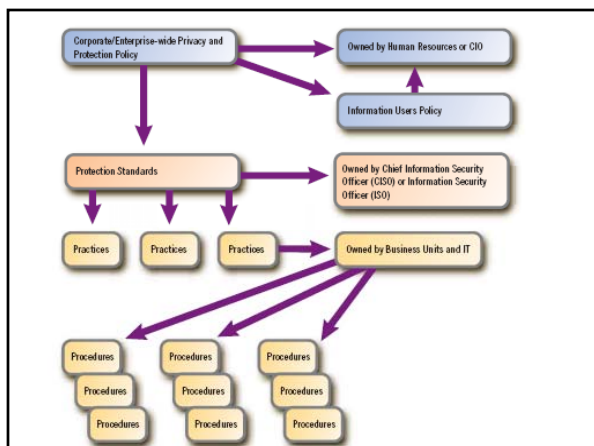
13 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

How a Policy Framework Works

- **Define Your Terms**
 - Policies
 - Standards
 - Guidelines, Practices and Procedures
- **Ownership and Custodial Responsibility**
 - Determine who will manage policy changes and implementation
- **Endorsement**
 - Determine who will act as the signing authority for various levels of documentation
- **Distribution**
 - Determine the appropriate communication channels, training methods and acknowledgement process

14 | 10/17/2008 | © 2008 IBM Corporation



Professional Security Services

Where to Start?

- **Obtain Support for the Project**
- **Collect all relevant security policy documentation**
 - Policies
 - Checklists
 - Procedures
 - De Facto Policy
- **Review current documentation practices**
- **Develop a documentation framework**

16 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

The Policy Development Process

Work from the top down – Polices and Standards need to be developed and approved first

- **Understand the organization's environment, technology infrastructure and risk model through interview sessions and data gathering**
- **Identify best practices from peer organizations**
- **Draft documentation**
- **Facilitate working review sessions to socialize and finalize documentation**
- **Develop implementation plans**

17 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Policy Implementation

- **Conduct a Gap Analysis between current operations and the newly approved policies and standards**
- **Identify those gaps that are either:**
 - Required by statute or regulation
 - Easy or inexpensive to implement
 - Create the greatest benefit to the organization's mission
- **Develop a phased implementation plan**
- **Exception out those policies/standards that can not be implemented in the next 12 months**

18 | 10/17/2008 | © 2008 IBM Corporation

Professional Security Services

Summary

- Policy is a critical component of any compliance initiative
- Most organizations have shortcomings in their information security documentation
- A tiered framework allows for an effective and manageable set of information security policies
- Policies must be endorsed, enforced and trained


19 | 10/17/2008 | © 2006 IBM Corporation

Professional Security Services

Thank You!!

20 | 10/17/2008 | © 2006 IBM Corporation

IBM Global Services



Policy Rules!

Building an Effective and Manageable Security Policy Framework

Steve Brown, CISSP-ISSMP
IBM Internet Security Systems

IBM Internet Security Systems
Ahead of the threat.™

10/17/2008 | © 2006 IBM Corporation
